(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106447310 A
(43)申请公布日 2017.02.22

(21)申请号 201610850482.9

(22)申请日 2006.09.28

(30)优先权数据
60/721,454 2005.09.28 US
60/807,775 2006.07.19 US

(62)分案原申请数据
200680043308.8 2006.09.28

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚

(72)发明人 T·希尔 J·S·萨霍塔
C·阿布耶 K·沃格纳
A·奥奇埃诺 C·奥本兰德
威廉·智渊·陈 C·A·格兰登宁

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 张劲松

(51)Int.Cl.
G06Q 20/04(2012.01)
G06Q 20/34(2012.01)
G06Q 20/36(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 30/06(2012.01)
G06K 7/00(2006.01)
G07F 7/08(2006.01)
G07F 7/10(2006.01)

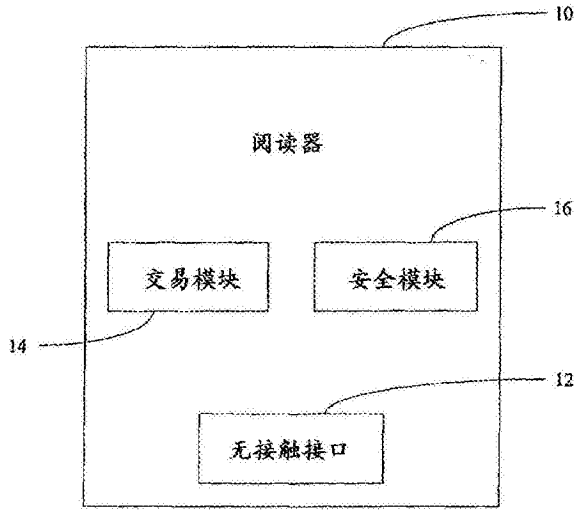
权利要求书3页 说明书7页 附图7页

(54)发明名称

减少无接触交易的交互时间的设备，系统和方法

(57)摘要

本发明公开了减少无接触交易的交互时间的设备，系统和方法。所述方法包括：在阅读器，在使无接触接口通电之前执行至少一种基于交易的风险管理处理，开始与用于无接触交易的卡的通信，接收和卡相关的信息，和在批准无接触交易之前终止与卡的通信。



CN 106447310 A

1.一种阅读器设备,包括:

无接触接口;

交易模块,该交易模块与所述无接触接口耦接,其中,所述交易模块被构造和安排成通过以下操作在无接触支付设备和阅读器之间小于1/2秒的交互时间内执行无接触交易:

从所述无接触支付设备请求无接触交易的动态签名验证;

从所述无接触支付设备接收具有动态签名的响应;以及

在接收具有动态签名的响应之后向所述无接触支付设备传送命令消息;和

安全模块,该安全模块与所述交易模块耦接,其中,所述安全模块被构造和安排成通过确认所述动态签名来防止对无接触交易数据的截取和更改。

2.根据权利要求1所述的阅读器,其中,所述阅读器被构造和安排成:

在对所述无接触交易授权之前终止与所述无接触支付设备的通信。

3.根据权利要求1所述的阅读器,其中,所述阅读器被构造和安排成:

接收基于应用交易计数器、终端不可预测数字和交易金额的密码;以及

如果所述动态签名未被确认,则借助所述密码请求在线处理交易。

4.根据权利要求1所述的阅读器,其中,所述交易模块还被构造和安排成:

从所述阅读器向无接触支付设备传送对于由所述无接触支付设备支持的、用于实施交易的应用的列表的请求。

5.根据权利要求1所述的阅读器,其中,所述交易模块被构造和安排成执行静态数据验证。

6.根据权利要求1所述的阅读器,其中,所述交易模块被构造和安排成执行动态数据验证。

7.一种阅读器设备,包括:

用于在无接触支付设备和所述阅读器设备之间小于1/2秒的交互时间内执行无接触交易的部件;

用于从所述无接触支付设备请求无接触交易的动态签名验证的部件;

用于从所述无接触支付设备接收具有动态签名的响应的部件;

用于在接收具有动态签名的响应之后向所述无接触支付设备传送命令消息的部件;

用于确认所述动态签名的部件。

8.根据权利要求7所述的阅读器设备,还包括:

用于在对所述无接触交易授权之前终止与所述无接触支付设备的通信的部件。

9.根据权利要求7所述的阅读器设备,还包括:

用于接收基于应用交易计数器、终端不可预测数字和交易金额的密码的部件;以及

用于如果所述动态签名未被确认、则借助所述密码请求在线处理交易的部件。

10.根据权利要求7所述的阅读器设备,还包括:

用于从所述阅读器向无接触支付设备传送对于由所述无接触支付设备支持的、用于实施交易的应用的列表的请求的部件。

11.根据权利要求7所述的阅读器设备,还包括:

用于执行静态数据验证的部件。

12.根据权利要求7所述的阅读器设备,还包括:

用于执行动态数据验证的部件。

13.根据权利要求7所述的阅读器设备，还包括：

用于将交易金额与预定值进行比较的部件。

14.根据权利要求7所述的阅读器设备，还包括：

用于接收与由所述无接触支付设备支持的至少一个应用相关联的信息的部件。

15.根据权利要求7所述的阅读器设备，还包括：

用于接收对于非金融交易的请求的部件。

16.一种用于减少无接触交易的交互时间的系统，包括：

卡；

阅读器，该阅读器包括：

无接触接口；

交易模块，该交易模块与所述无接触接口耦接，其中，所述交易模块被构造和安排成通过以下操作在所述卡和阅读器之间小于1/2秒的交互时间内执行无接触交易：

从所述卡请求无接触交易的动态签名验证；

从所述卡接收具有动态签名的响应；以及

在接收具有动态签名的响应之后向无接触支付设备传送命令消息；和

安全模块，该安全模块与所述交易模块耦接，其中，所述安全模块被构造和安排成通过确认所述动态签名来防止对无接触交易数据的截取和更改。

17.根据权利要求16所述的系统，其中，所述阅读器被构造和安排成：

在对所述无接触交易授权之前终止与所述卡的通信。

18.根据权利要求16所述的系统，其中，所述阅读器还被构造和安排成：

接收基于应用交易计数器、终端不可预测数字和交易金额的密码；以及

如果所述动态签名未被确认，则借助所述密码请求在线处理交易。

19.根据权利要求16所述的系统，其中，所述交易模块还被构造和安排成：

从所述阅读器向卡传送对于由所述卡支持的、用于实施交易的应用的列表的请求。

20.根据权利要求16所述的系统，其中，所述交易模块被构造和安排成执行静态数据验证。

21.根据权利要求16所述的系统，其中，所述交易模块被构造和安排成执行动态数据验证。

22.根据权利要求16所述的系统，其中，所述卡被构造和安排成通过所述无接触接口与阅读器通信，并且所述卡包括：

安全模块，该安全模块被构造和安排成与所述阅读器协作以防止对无接触交易数据的截取和更改；和

交易模块，该交易模块被构造和安排成与所述阅读器协作以执行无接触交易。

23.根据权利要求16所述的系统，其中，所述卡还被构造和安排成：

在执行在线交易之前终止所述阅读器和卡之间的通信。

24.根据权利要求22所述的系统，其中，所述卡还被构造和安排成：

生成基于应用交易计数器、终端不可预测数字和交易金额的应用密码。

25.根据权利要求22所述的系统，其中，所述卡还被构造和安排成：

使应用交易计数器递增。

26.根据权利要求16所述的系统，其中，所述卡还被构造和安排成按照磁条模式或者用于无线通信的芯片模式工作。

27.一种用于减少无接触交易的交互时间的方法，包括：

从无接触支付设备接收用于发起无接触交易的请求；

从所述无接触支付设备请求无接触交易的动态签名验证；

从所述无接触支付设备接收包含动态签名的响应；

响应于接收到所述动态签名而向所述无接触支付设备传送命令消息；以及

确认所述动态签名，

其中，所述方法在0.5秒内被执行。

28.根据权利要求27所述的方法，还包括：

从所述无接触支付设备接收基于应用交易计数器、终端不可预测数字和交易金额的密码；以及

在确认所述动态签名失败时借助所述密码请求在线处理交易。

29.根据权利要求27所述的方法，其中，所述动态签名在不需要与所述无接触支付设备进一步通信的情况下被确认。

30.根据权利要求27所述的方法，其中，所述命令消息包括记录请求，并且其中，确认所述动态签名基于在所述支付设备中的位置处被访问的请求的记录。

31.根据权利要求27所述的方法，还包括：

向所述无接触支付设备提供不可预测数字，其中，所述动态签名由所述无接触支付设备至少部分地基于所述不可预测数字来生成。

减少无接触交易的交互时间的设备,系统和方法

[0001] 本申请是基于申请号为200680043308.8、申请日为2006年9月28日、发明名称为“减少无接触交易的交互时间的设备,系统和方法”的专利申请的分案申请。

[0002] 交叉申请的相关引用

[0003] 本申请要求2005年9月28日提出的美国临时专利申请No.60/721,454和2006年7月19日提出的美国临时专利申请No.60/807,775的优先权。

技术领域

[0004] 本申请公开一种涉及减少无接触交易的交互时间的设备,系统和方法。

背景技术

[0005] 近年来,无接触和无线通信技术已变得更加普遍。在支付产业中,无接触支付具有优于传统的磁条技术和接触式芯片支付协议两者的许多优点。例如,已知传统的接触式支付卡操作相当缓慢,磁条卡不够安全。这些技术还都需要必须由商家维护的终端阅读器中的插槽。

[0006] 无接触支付不需要插入支付卡的插槽。消费者保持对支付卡的控制,需要时仅仅把支付卡放置在终端阅读器附近。支付产业就接触式芯片支付所采用的传统规范一般要求消费者在不同的时间和/或持续延长的一段时间把支付卡放置在终端阅读器附近,以便完成交易。由于商家和消费者都希望交易时间短,因此按照传统规范执行的无接触交易不能满足市场要求。

[0007] 商家和消费者还要求无接触交易更安全。尽管最新发行的无接触磁条卡能够比传统的磁条卡更安全,不过这种无接触磁条卡一般只是为在线交易设计的。对于按照传统规范执行的无接触在线交易,交易易受通常称为隐藏攻击(sleeve attack)、特洛伊木马攻击等的各类在线“中间人”攻击影响。

[0008] 在一种隐藏攻击中,设备截取从供无接触卡用的读卡器无线传送的数据。设备变更该数据,随后把变更的数据传给该卡。卡接收由设备传送的变更数据,而不是接收读卡器传送的数据。卡随后处理变更的数据,并把与变更数据相关的消息传给读卡器。读卡器随后根据存在于卡传送的消息中的信息,批准交易。在另一种隐藏攻击中,设备截取从供读卡器用的卡无线传送的数据。设备变更该数据,随后把变更的数据传给读卡器。读卡器接收由设备传送的变更数据,而不是接收卡传送的数据。读卡器随后处理变更的数据,并根据存在于设备传送的变更数据中的信息,批准交易。在其它类型的隐藏攻击中,通过不把截取的数据转发给卡或读卡器,设备可导致服务的拒绝。

[0009] 在一种特洛伊木马攻击中,在信息被发给读卡器之前,嵌入卡中的恶意软件变更有效数据。读卡器最终根据变更的数据批准交易。在另一种特洛伊木马攻击中,嵌入卡中的恶意软件在授权过程之前变更有效数据。读卡器最终根据变更的数据批准交易。

[0010] 对于指定的离线交易,“中间人”攻击可被用于减少最终由卡和读卡器识别的交易的金额。例如,对于涉及从商家购买商品的指定离线交易,读卡器可无线传送预定给卡的数

据，所述数据指示交易的价格等于$15。但是，在卡收到数据之前，设备截取所述数据，并变更该数据，以致变更的数据指示交易的价格仅仅等于$1。一旦卡随后收到变更的数据，并把与变更数据相关的消息传给读卡器，读卡器随后就批准仅仅等于$1的交易。当收到所述批准时，在相信批准的交易金额等于$15的情况下，商家发出商品。实际交易金额和减少的交易金额之间的差值会影响商家最终从发卡机构收到的金额。

发明内容

[0011] 在一个方面，本申请公开一种阅读器。按照各个实施例，所述阅读器包括无接触接口和交易模块。交易模块与无接触接口耦接，并被构造和安排成以卡和阅读器之间小于1/2秒的交互时间处理无接触交易。

[0012] 在另一方面，本发明公开一种卡。按照各个实施例，所述卡包括构造和安排成进行无线通信的交易模块，所述卡被构造和安排成按照芯片模式和磁条数据模式工作。

[0013] 在另一方面，本发明公开一种系统，按照各个实施例，所述系统包括阅读器和卡。阅读器包括无接触接口和交易模块。卡被构造和安排成通过无接触接口与阅读器通信。交易模块与无接触接口耦接，并被构造和安排成以卡和阅读器之间小于1/2秒的交互时间处理无接触交易。

[0014] 在另一方面，本申请公开一种减小无接触交易的交互时间的方法。按照各个实施例，所述方法包括：在所述阅读器，在使无接触接口通电之前执行至少一种基于交易的风险管理处理，开始与用于无接触交易的卡的通信，接收和卡相关的信息，在批准无接触交易之前终止与卡的通信。

[0015] 在另一方面，本申请公开一种防止对无接触交易的中间人攻击的方法。按照各个实施例，所述方法包括接收动态签名，所述动态签名包括应用交易计数器、终端不可预测数字、交易金额、交易货币代码和卡不可预测数字。所述方法还包括接收卡不可预测数字，利用卡不可预测数字重新计算动态签名，和如果动态签名被确认，那么离线批准无接触交易。

[0016] 本发明的各个方面可由计算设备和/或保存在计算机可读介质上的计算机程序实现。计算机可读介质可包括磁盘，设备和/或传播信号。

附图说明

[0017] 下面结合附图，举例说明本发明的各个实施例。

[0018] 图1图解说明减少无接触交易的交互时间的阅读器的各个实施例；

[0019] 图2图解说明减少无接触交易的交互时间的系统的各个实施例；

[0020] 图3图解说明减少无接触交易的交互时间的方法的各个实施例；

[0021] 图4是图解说明图3的方法的初步交易处理步骤的各个实施例的简化流程图；

[0022] 图5是图解说明图3的方法的应用选择步骤的各个实施例的简化流程图；

[0023] 图6是图解说明图3的方法的授权步骤的各个实施例的简化流程图；

[0024] 图7图解说明用于减少第二无接触交易的交互时间的方法的各个实施例。

具体实施方式

[0025] 要明白本发明的至少一些附图和说明已被简化，以便集中在与清楚地理解本发明

相关的要素上，同时为了清楚起见，消除了本领域的普通技术人员会认识到也可构成本发明的一部分的其它要素。但是，由于这样的要素在本领域中众所周知，并且由于它们不一定帮助更好地理解本发明，因此这里省略对这种要素的说明。

[0026] 图1图解说明用于减少无接触交易的交互时间的阅读器10的各个实施例。阅读器10可以是被构造和安排成通过无接触接口与另一设备通信的任意类型的设备。按照各个实施例，阅读器10可以是集成到销售点设备中的商业设备，或者与销售点设备分离，但是与销售点设备通信的商业设备。这里使用的术语“交互时间”指的是阅读器10和另一设备之间的交互时间，并不包括为了授权而上线，或者阅读器确认静态或动态签名以便进行离线数据验证所需的时间。阅读器10可以和要求交易时间比与传统的支付协议相关的交易时间更快的市场的现有支付系统基础设施一起使用。按照各个实施例，阅读器10可被用于把交互时间降低到大约小于500毫秒。

[0027] 阅读器10包括无接触接口12，和与无接触接口耦接的交易模块14。交易模块14被构造和安排成以阅读器10和另一设备之间小于1/2秒的交易时间处理无接触交易。交易模块14还可被构造和安排成执行静态数据验证和/或动态数据验证，如下更详细所述。按照各个实施例，阅读器10还包括与交易模块14耦接的安全模块16。安全模块16被构造和安排成阻止对无接触交易的“中间人”攻击。

[0028] 模块14、16都可用硬件或软件实现。按照各个实施例，通过利用任何合适的计算机语言(例如，C，C++，Delphi，Java，JavaScript，Perl，Visual Basic，VBScript等)，模块14、16可被实现成应用软件，计算机程序等等，并且可被永久或者暂时包含在能够向设备传递指令的任意类型的机器，组件，物理或者虚拟设备，存储介质，或者传播信号中。软件代码可以一系列的指令或命令的形式被保存在计算机可读介质上，以致当处理器读取所述介质时，执行这里描述的功能。这里使用的术语“计算机可读介质”包括磁和光存储器，比如磁盘，只读光盘，可写光盘，光盘驱动器和硬盘驱动器。计算机可读介质还包括可以是物理的，虚拟的，永久的，临时的，半永久和/或半临时存储装置。计算机可读介质还可包括一个或多个传播信号，这样的传播信号可在一个或多个载波上传送，或者可不在一个或多个载波上传送。尽管模块14和16在图1中被表示成两个独立模块，不过本领域的技术人员会认识到模块14和16的功能可被结合到单一模块中。

[0029] 图2图解说明用于减少无接触交易的交易时间的系统20的各个实施例。系统20包括阅读器10和卡22。这里使用的术语“卡”指的是能够通过无接触接口12与阅读器10通信的任意类型的设备。按照各个实施例，卡22可以是智能卡，移动电话机，个人数字助手等等。卡22被构造和安排成通过无接触接口12与阅读器10通信。按照各个实施例，卡22包括交易模块24，交易模块24被构造和安排成与阅读器10协作，以完成无接触交易。卡22还可包括安全模块26，安全模块26被构造和安排成与阅读器10协作，以阻止对无接触交易的“中间人”攻击。模块24，26可以类似于阅读器10的模块14，16。按照各个实施例，卡22可以是双模卡，所述双模卡可被构造和安排成按照芯片模式，或者按照磁条数据模式(利用Track 2等效数据)工作。卡22利用的工作模式可由卡22根据阅读器10的能力来确定。

[0030] 系统20还可包括和阅读器20和发卡机构(issuer)30耦接的网络28。网络28可以是本领域中已知的任何合适类型的网络，可以按照本领域已知的任何适当方式与阅读器28耦接，可以按照本领域已知的任何适当方式与发卡机构30耦接。网络28可以包括任何类型的

传输系统，包括(但不限于)局域网(例如，以太网)，广域网(例如因特网和/或万维网)，电话网(例如，模拟，数字，有线，无线，PSTN，ISDN，GSM，GPRS和/或xDSL)，分组交换网，无线电网络，电视网络，电缆网，卫星网络，和/或配置成传送数据的任何其它有线或无线通信网络。网络28可以包括配置成引导和/或传送数据的多个部件，比如中间节点，代理服务器，路由器，交换机和适配器。

[0031] 图3图解说明用于减少无接触交易的交互时间的方法40的各个实施例。方法40可由图2的系统20实现。方法40包括通用步骤：初步交易处理42，发现处理4，应用选择46，应用处理48，和交易授权50。

[0032] 为了使指定交易的卡22和阅读器之间的交互时间降至最小，在请求呈递卡22之前，阅读器10执行初步交易处理步骤42。在初步交易处理步骤42中，阅读器10执行某些基于交易的风险管理处理。例如，按照各个实施例，阅读器10可获得交易金额，并比较交易金额与交易限额，免授权限额(floor limit)，持卡人核实方法限额等等。一旦初步交易处理步骤42完成，阅读器10可提示持卡人呈递卡22。根据初步交易处理，阅读器10可要求交易被终止，在线处理或者离线处理。图解说明初步交易处理步骤42的各个实施例的简化流程图示于图4中。

[0033] 初步交易处理步骤42之后是发现处理步骤44。一旦卡22被呈递，并且在阅读器10的范围之内，阅读器10使无接触接口12通电，并在发现处理步骤44期间通过无接触接口12与卡22建立通信。如果阅读器10在其范围内检测到多个无接触卡22，那么阅读器10可向持卡人指出该情况，并要求只为该交易呈递一张卡22。另外，依据商家命令或者在预定超时时段之后，阅读器10可在发现处理步骤44期间异常终止交易，并使无接触接口12断电。

[0034] 发现处理步骤44之后是应用选择步骤46。在应用选择步骤46中，阅读器10向卡22传送第一命令消息(例如，SELECT PPSE)。第一命令消息可用作对卡22支持的，并且可通过无接触接口12访问的应用的应用标识符，应用标签和应用优先级指示符的列表的请求。响应第一命令消息，卡22建立这样的列表，并把该列表传给阅读器10。按照各个实施例，可在传给阅读器10的文件控制信息(FCI)内提供该列表。阅读器10随后利用卡22传送的列表建立为阅读器10和卡22所共有的应用的列表。在建立共有应用的列表之后，阅读器10向卡22传送第二命令消息(例如，SELECT AID)。第二命令消息可用作利用出自共用应用列表中的特定应用，实施交易的请求。按照各个实施例，所述特定应用可以是由卡22先前传送的应用优先级指示符指示的具有最高优先级的共有应用。响应第二命令消息，卡22向阅读器10传送提供和阅读器10的能力，以及阅读器10的交易特殊要求有关的各种细节的请求。按照各个实施例，可用与阅读器10相关的终端数据对象列表(例如PDOL)提供所请求的细节。如果终端数据对象列表包括特殊的数据元素(例如，终端交易限定符(qualifier))，那么处理进入应用处理步骤48。否则，阅读器10可以终止交易，或者试图通过另一接口处理交易。图解说明应用选择步骤46的各个实施例的简化流程图示于图5中。

[0035] 在应用处理步骤48中，响应卡对与阅读器10的能力，以及阅读器10的交易特殊要求有关的各种细节的请求，阅读器10向卡22传送第三命令消息(例如，GPO)。第三命令消息被这样构成，以致能够利用它代替以前的规范所要求的三个独立命令。通过减少完成无接触交易所需的命令和响应的数目，卡22和阅读器10之间所需的交互时间被进一步最小化。第三命令消息可包括卡22请求的许多数据元素的值。各个数据元素值指示阅读器10支持的

交易的类型，阅读器10是否支持或要求离线和/或在线处理，阅读器10支持或要求哪些持卡人核实方法，等等。数据元素可包括终端交易限定符，交易金额，终端不可预测数字，交易货币代码，和卡22在其对第二命令消息的响应中所请求的任何其它数据。

[0036] 根据阅读器10支持的交易的类型，卡22随后执行与特定的交易类型关联的许多风险管理处理。按照各个实施例，风险管理处理可包括检查内部卡指示符以免交易风险(tearing)，比较应用货币代码的值与交易货币代码的值，比较个人识别号码条目的数目与预定极限，确定是否要求持卡人核实方法，比较交易金额和与卡22相关的低值限度(low value limit)，比较交易金额和与卡22相关的累积交易总金额，比较连续交易计数器的值与连续交易限度的值等等。通过在交易中的这一时刻执行引用的风险管理处理，与按照传统规范在稍后的时刻执行风险管理处理相反，卡22和阅读器10之间的交互时间被进一步最小化。根据风险管理处理，卡22可请求终止交易，在线处理交易，或者离线处理交易。

[0037] 在完成风险管理处理之后，卡22建立对第三命令消息的适当响应，并把该响应传给阅读器10。包括在该响应中的信息可随卡22是要求交易被在线批准，离线批准，还是被终止而变化。例如，当卡22要求交易被在线批准时，所述响应可包括指示卡处理的交易的数目的应用交易计数器(ATC)，由卡22利用应用交易计数器和包括在第三命令消息中的终端数据(例如，终端不可预测数字和交易金额)产生的应用密码，指示支持风险管理功能的应用交互特征(AIP)(application interchange profile)，发卡机构应用数据，Track 2等效数据，以及各种其它数据元素。

[0038] 当卡22要求交易被离线批准时，对第三命令消息的响应可包括指示卡所处理的交易的数目的应用交易计数器(ATC)。所述响应还可包括卡22利用应用交易计数器，包括在第三命令消息中的终端数据(例如，终端不可预测数字，交易金额，和交易货币)，以及卡不可预测数字产生的动态签名。所述响应还包括卡22利用应用交易计数器和包括在第三命令消息中的终端数据(例如，终端不可预测数字和交易金额)产生的应用密码。另外，所述响应可包括指示与应用相关的文件和记录的位置的应用文件定位器(AFL)，指示支持风险管理功能的应用交互特征(AIP)，发卡机构应用数据，和各种其它数据元素。按照各个实施例，在计算应用密码和动态签名之前，卡22可以递增应用交易计数器。如果动态签名的大小超过预定阈值，那么可响应下面说明的第四命令消息，在授权步骤50中返回动态签名。按照各个实施例，卡22产生的应用密码包括与以前的规范所利用的应用密码相比，更少的数据元素。通过利用更少的数据元素来产生应用密码，总的处理时间被减少，卡22和阅读器10之间的交互时间被进一步最小化。

[0039] 应用处理步骤48之后是授权步骤50。在阅读器10从卡22收到对第三命令消息的响应之后，当要在线批准交易时，可从阅读器10的范围内移除卡22。于是，在请求并执行在线授权的时候，不要求卡22保持在阅读器10的范围内。由于能够在交易处理中的这一时刻移除卡22，卡22和阅读器10之间的交互被进一步最小化。阅读器10随后把卡22响应第三命令消息提供的应用密码在线提供给发卡机构30。根据随后从发卡机构30收到的响应，阅读器批准或者拒绝交易。

[0040] 当交易要被离线批准时，在从卡22收到对第三命令消息的响应之后，阅读器10向卡22传送第四命令消息(例如，READ RECORD)。第四命令消息可用作对在卡22响应第三命令消息提供的应用文件定位器(AFL)中指示的记录的请求。响应第四命令消息，卡22把合适的

记录传给阅读器10。当阅读器10收到最后一条记录时，可从阅读器10的范围内移除卡22。于是，在进行离线授权的时候，不要求卡22保持在阅读器10的范围内。由于能够在交易处理中的这一时刻移除卡22，卡22和阅读器10之间的交互被进一步最小化。阅读器10随后检查卡22是否到期。如果阅读器10确定卡22未到期，那么阅读器10随后进行离线数据验证。所执行的离线数据验证的类型，静态数据验证(SDA)或动态数据验证(DDA)是根据卡22响应第三命令消息提供的应用交互特征(AIP)确定的。

[0041] 对于静态数据验证来说，阅读器10试图确认卡22响应第三命令消息提供的静态签名。静态数据验证涉及确认重要的应用数据，以保证数据未被欺诈性地变更。如果静态签名被确认，那么交易被离线批准。否则，交易可被在线发送或者终止。对于动态数据验证来说，阅读器10试图确认卡22响应第三命令消息提供的动态签名。动态数据验证涉及确认重要的应用数据，以保证数据未被欺诈性地变更，以及卡22是真实的。按照各个实施例，动态签名的确认可包括利用卡22响应第三命令消息提供的应用交易计数器(ATC)和终端不可预测数字来重新计算动态签名。按照其它实施例，动态签名的确认可包括利用从卡接收的卡不可预测数字重新计算动态签名。如果动态签名被确认，那么阅读器10产生结算消息，所述结算消息包括卡22响应第三命令消息提供的密码，以及其它相关数据。否则，交易可被在线发送或者终止。按照各个实施例，如果动态签名未被确认，那么阅读器10可利用先前从卡22接收的密码在线发送交易。从而，阅读器10可利用离线密码产生一个在线请求。图解说明授权步骤50的各个实施例的简化流程图示于图6中。

[0042] 如上所述，方法40可被用于使无接触交易的卡22和阅读器10之间的交互时间减到最小，以小于大约500毫秒。为了防止对无接触交易的离线隐藏攻击，方法40的各个实施例可利用一种新颖的动态数据验证。对于离线交易来说，卡22可利用应用交易计数器(ATC)和卡不可预测数字，以及包括在第三命令消息(例如，GPO)中的终端不可预测数字，交易金额和交易货币代码来产生动态签名。随后响应第三命令消息和动态签名一起发给阅读器10的应用文件定位器(AFL)指向包含RSA证书和与动态数据验证相关的数据的记录。于是，在验证步骤50中，阅读器10可读取发卡机构证书，无接触卡证书，和与动态数据验证有关的数据。按照各个实施例，阅读器10可利用响应第四命令消息，从卡22接收的应用交易计数器(ATC)，卡不可预测数字，终端不可预测数字，交易金额和交易货币代码，重新计算供确认之用的动态签名。在无接触交易受到隐藏攻击的情况中，重新计算不会匹配先前从卡22接收的动态签名。对于这种情况，阅读器10可拒绝或终止无接触交易。

[0043] 图7图解说明减少在对方法40的在线授权的请求之后发生的第二无接触交易的交互时间的方法60的各个实施例。按照各个实施例，方法60可包括方法40的一部分。方法60可由图2的系统20实现。方法60可被用于使第二无接触交易的卡22和阅读器10之间的交互时间降至最小，小于大约500毫秒。按照各个实施例，方法60包括通用步骤：第二交易请求62，应用选择4，应用处理66，和交易批准68。

[0044] 第二无接触交易不是金融交易。由于第二无接触交易包括在阅读器10的范围内持续第二时间呈递卡22，因此该处理可被称为卡返回处理。在开始该处理之前，在上面说明的第一交易中，阅读器10和卡22都可相互指出它们支持卡返回处理。例如，阅读器10和卡22可在第一交易的应用选择步骤46中指出它们对卡返回处理的支持。

[0045] 在方法40的步骤50请求在线授权之后，阅读器10或卡22(通过持卡人)可在第二交

易请求步骤62请求第二无接触交易。按照各个实施例，当对在线授权请求的发卡机构响应包括将被传给卡22的消息时，阅读器10可在第二交易请求步骤62内请求第二无接触交易。这样的消息可被用于向卡22提供更新或计数器复位，或者封存帐户。例如，在在线授权响应中，发卡机构30可在该响应中包括要求持续第二时间呈递卡22的脚本消息。这样，发卡机构30随后能够封存帐户，补充离线消费能力，增加离线消费额度等等，即使卡22没有请求采取这样的行动。为了提示持卡人持续第二时间呈递卡22，阅读器10可以显示指出需要另外的卡处理时间的消息，请求再次呈递卡的消息，等等。

[0046] 按照其它实施例，当卡离线消费能力变低时，卡22可请求第二交易，以便接收增值(reload)。例如，当卡离线消费能力变低时，通过持卡人，卡22可通过请求在线授权，并提供当前的可用消费金额，请求续费。为了保证卡22是对于第一交易呈递的同一张卡22，在第二交易请求步骤62中可以验证卡22。

[0047] 第二交易请求步骤62之后是应用选择步骤64。方法60的应用选择步骤64类似于上面说明的方法40的应用选择步骤46。在应用选择步骤64中，阅读器10向卡22传送命令消息(例如，SELECT VSDC AID)。该命令消息可以用作利用出自阅读器10先前建立的共用应用列表的特定应用，实施第二交易的请求。响应该命令消息，卡22向阅读器10传送PDOL。PDOL可以类似于在上面说明的方法40的应用选择步骤46中传送给阅读器10的PDOL。如果PDOL包括特定的数据元素(例如，终端交易限定符)，那么处理进入应用处理步骤66。

[0048] 应用处理步骤66在应用选择步骤64之后。应用处理步骤66可以类似于上面说明的方法40的应用处理步骤48，不过不同之处在于不涉及任何金融交易处理。在应用处理步骤66中，阅读器10向卡22传送另一命令消息(例如，GPO)。当收到该命令消息时，卡22建立适当的响应，并把该响应传给阅读器10。

[0049] 应用处理步骤66之后是交易批准步骤68。按照各个实施例，如果发卡机构30决定增值与卡22相关的离线消费能力，那么发卡机构30可传送响应密码，并批准交易或者借助消息验证代码(MAC)包括脚本消息。密码或MAC可用于保证只对与发卡机构30相关的卡22进行更新，计数器复位等等。

[0050] 如上所述，方法60可被用于改变卡风险参数，卡计数器，卡状态等等。例如，就改变卡风险参数来说，方法60可被用于增大离线消费额度，增大单次交易额度，允许卡用两种或者更多的不同货币进行交易，改变采用的货币兑换率等等。就改变卡计数器来说，方法60可被用于使离线可用消费金额复位，等等。就改变卡状态来说，方法60可被用于封锁或者解锁特定的应用。本领域的技术人员会认识到方法60可被用于改变其它参数，计数器等等。

[0051] 尽管这里举例说明了本发明的几个实施例，不过本领域的技术人员会认识到可以实现对所述实施例的各种修改，变更和适应，而不脱离由附加权利要求限定的本发明的精神和范围。例如，按照各个实施例，上面说明的阅读器10，系统20和/或方法40可被修改，以阻止对利用信息的无线传输的无线手持机，USB欺诈(fob)和其它设备的类似类型的“隐藏攻击”。另外，方法60的各个实施例可被用于处理与货币兑换，忠诚度计划等相关的交易。

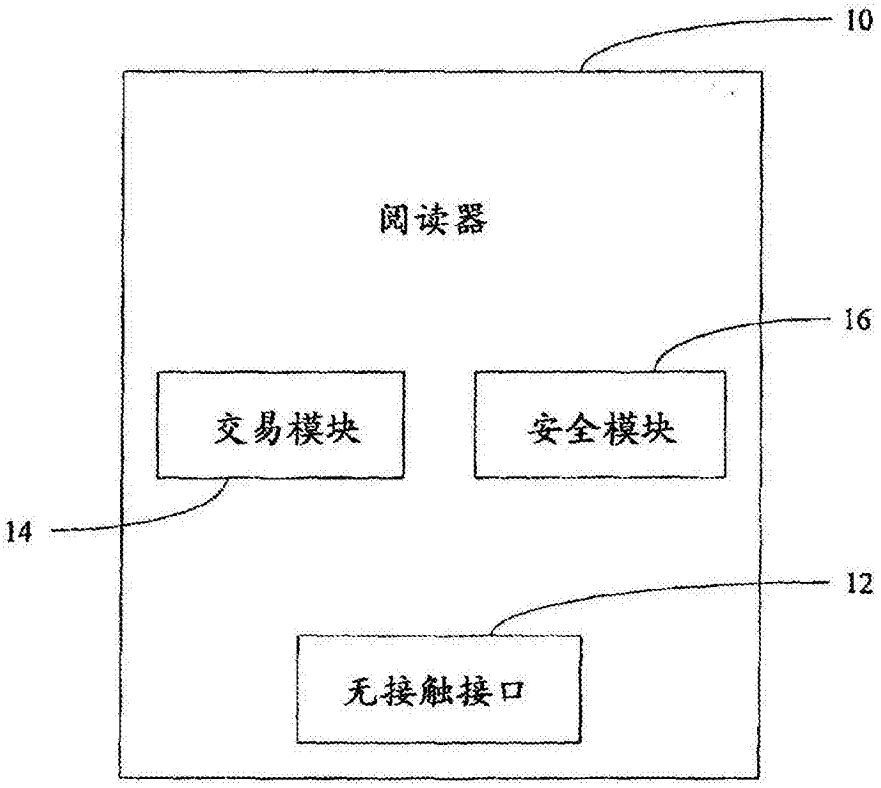


图1

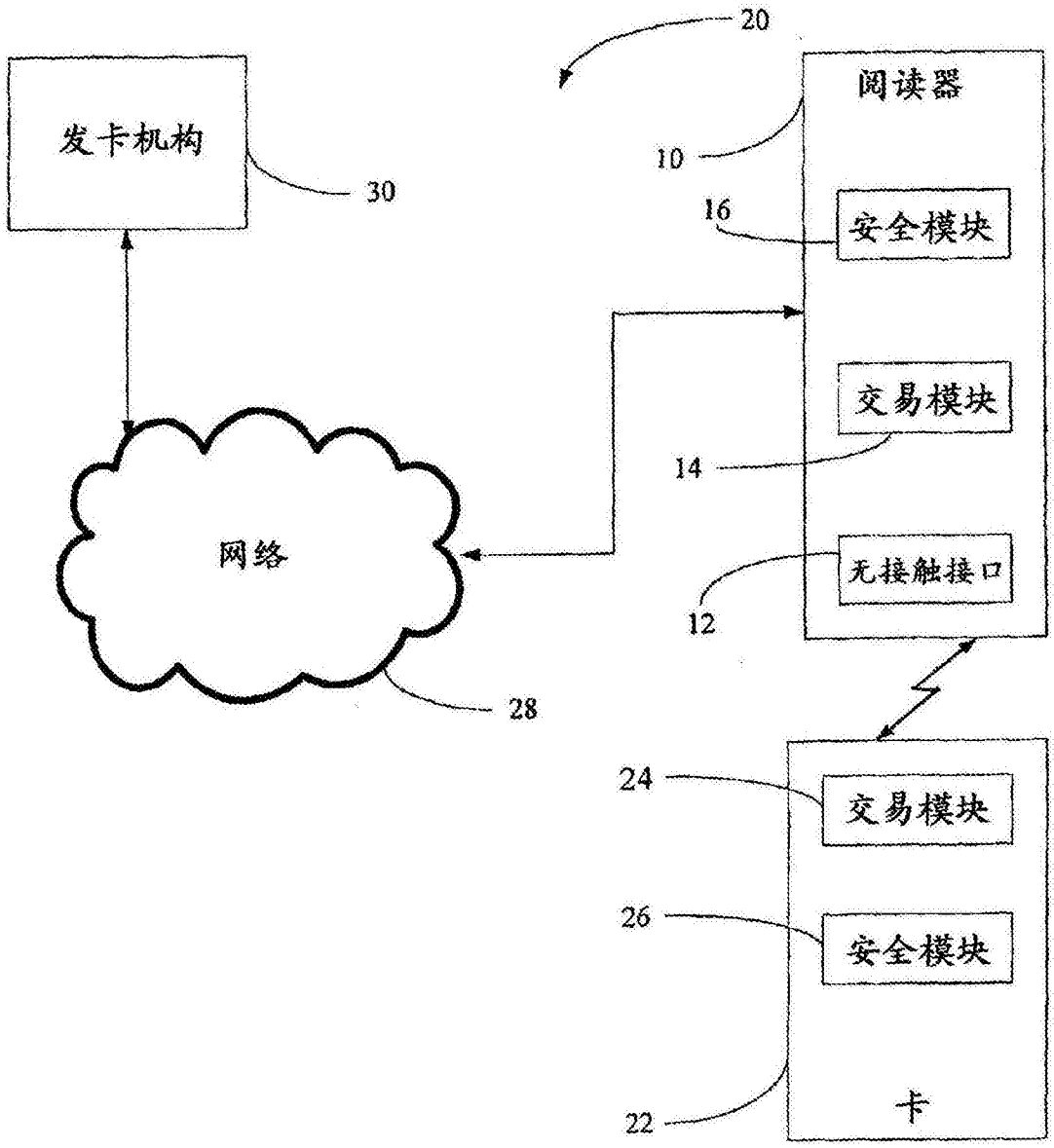

20
发卡机构
30
阅读器
10
16
安全模块
交易模块
14
网络
无接触接口
12
28
24
交易模块
26
安全模块
卡
22

图2

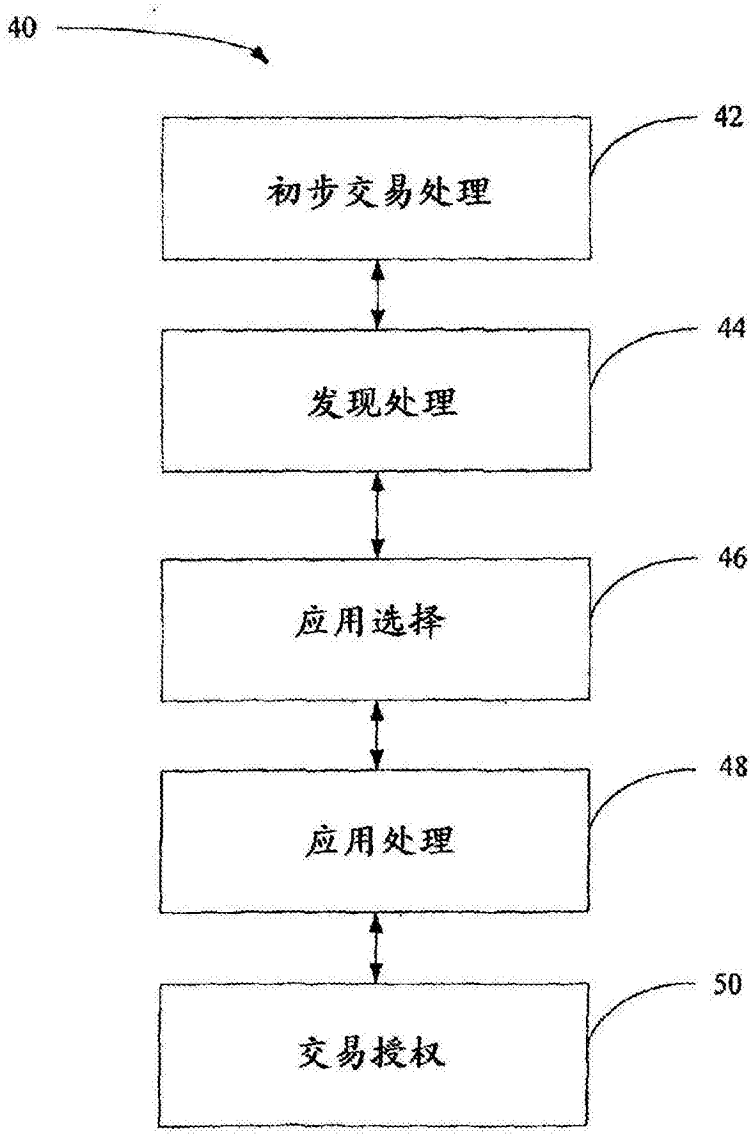


图3

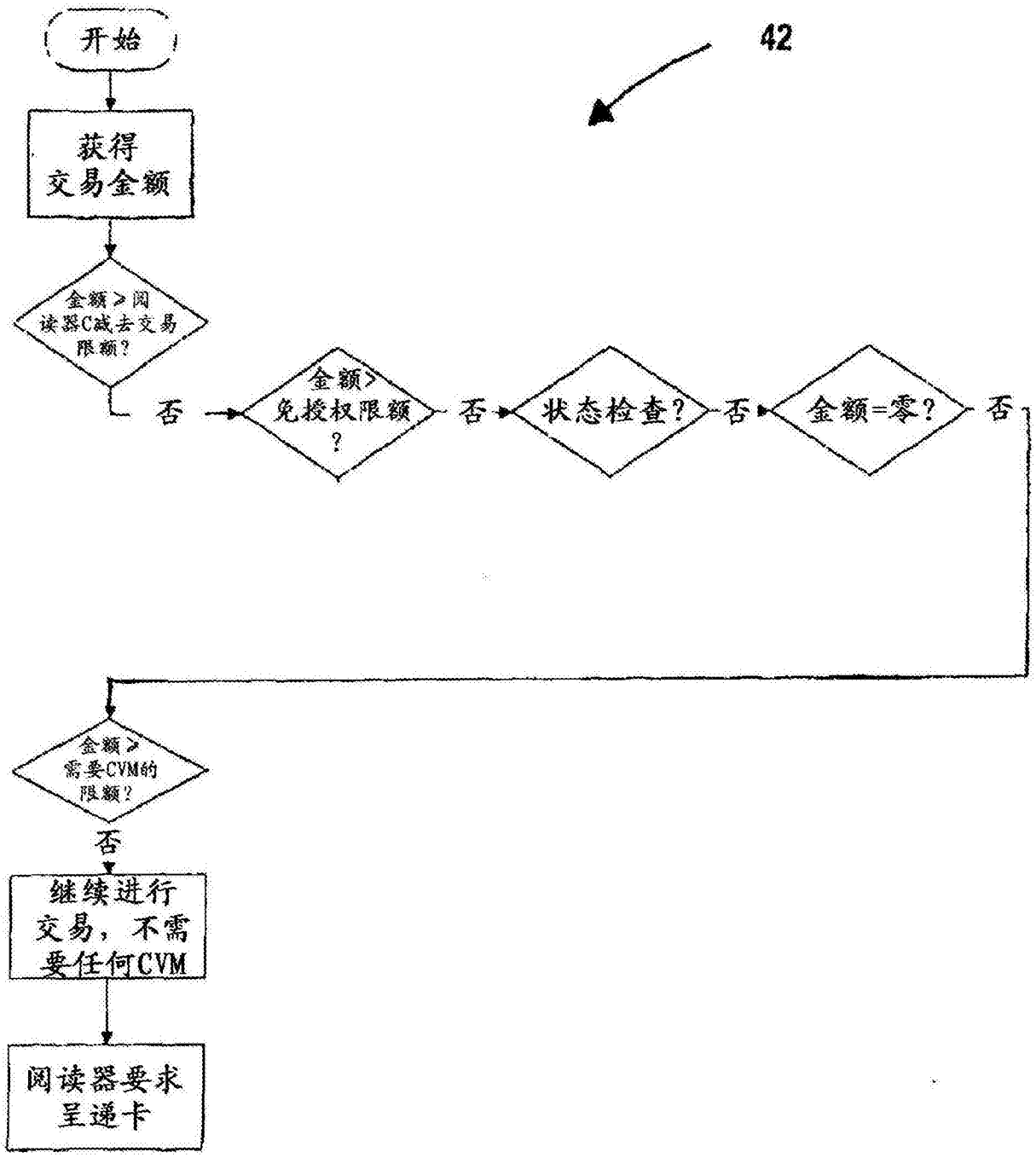

开始
42
获得交易金额
金额≥阅读器C减去交易限额?
否
金额>免授权限额?
否
状态检查?
否
金额=零?
否
金额>需要CVM的限额?
否
继续进行交易，不需要任何CVM
阅读器要求呈递卡

图4

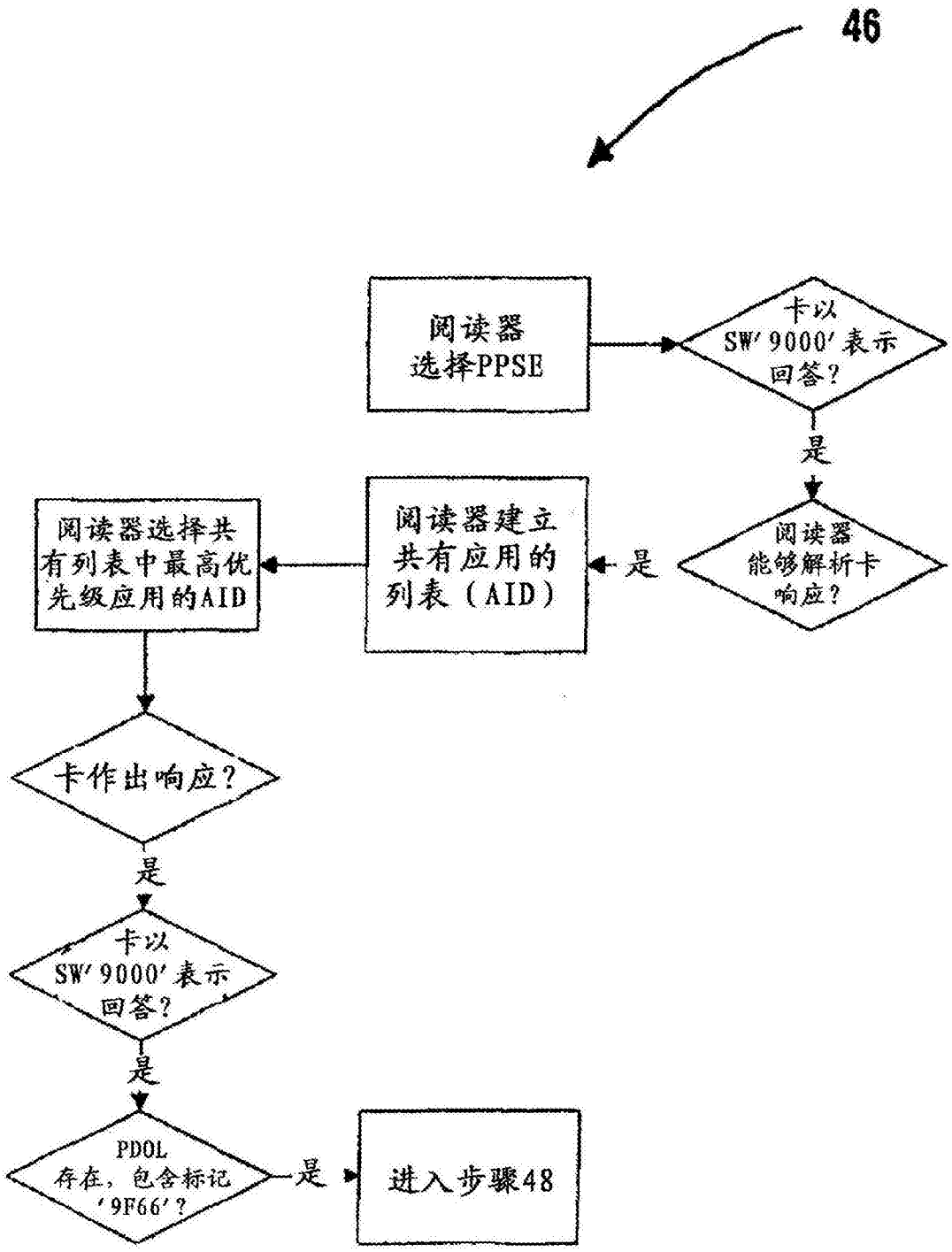

46
阅读器
选择PPSE
卡以
SW'9000'表示
回答?
是
阅读器
能够解析卡
响应?
是
阅读器建立
共有应用的
列表（AID）
阅读器选择共
有列表中最高优
先级应用的AID
卡作出响应?
是
卡以
SW'9000'表示
回答?
是
PDOL
存在，包含标记
'9F66'?
是
进入步骤48

图5

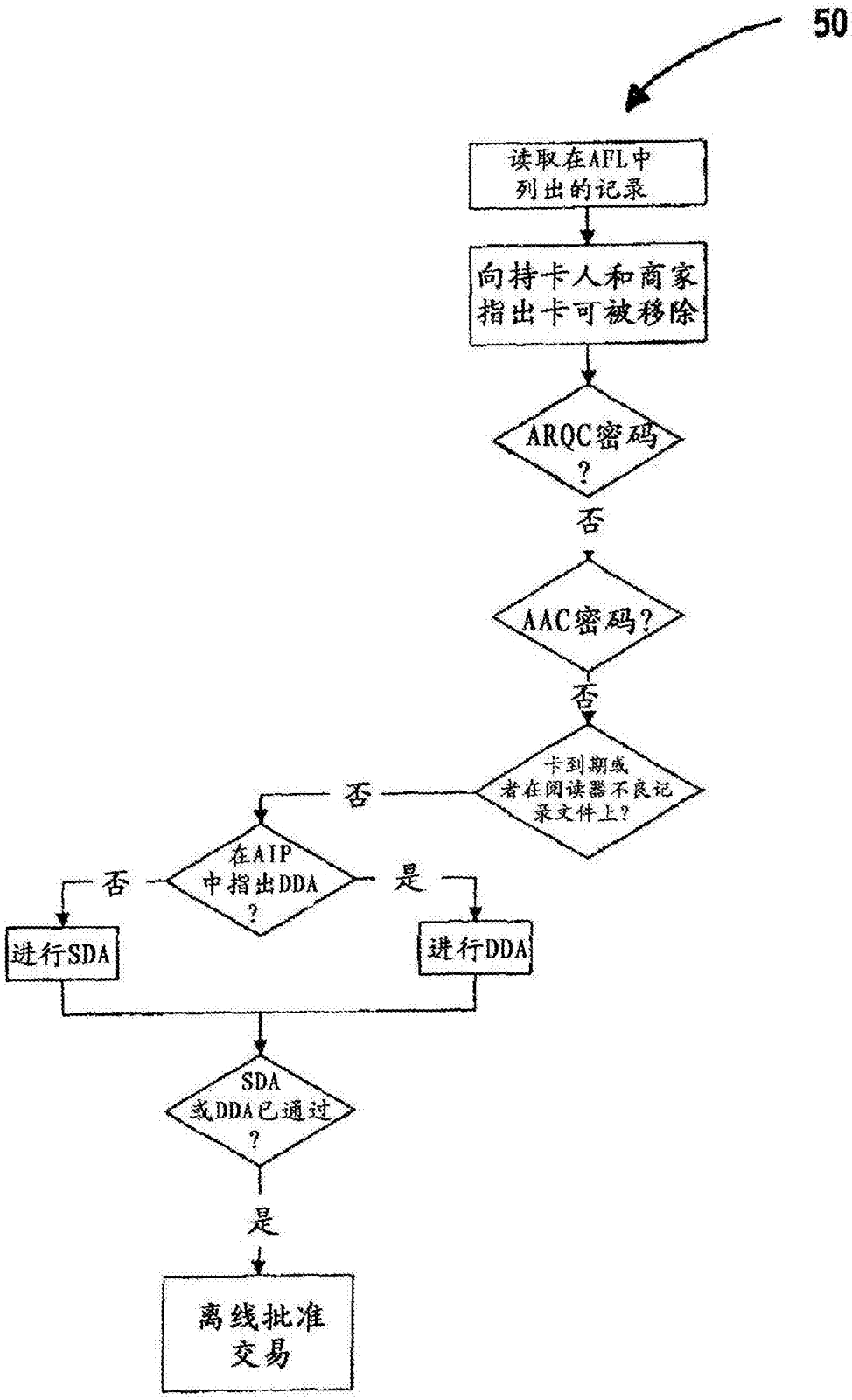

50
读取在AFL中列出的记录
向持卡人和商家指出卡可被移除
ARQC密码?
否
AAC密码?
否
卡到期或者在阅读器不良记录文件上?
否
在AIP中指出DDA?
否
是
进行SDA
进行DDA
SDA或DDA已通过?
是
离线批准交易

图6

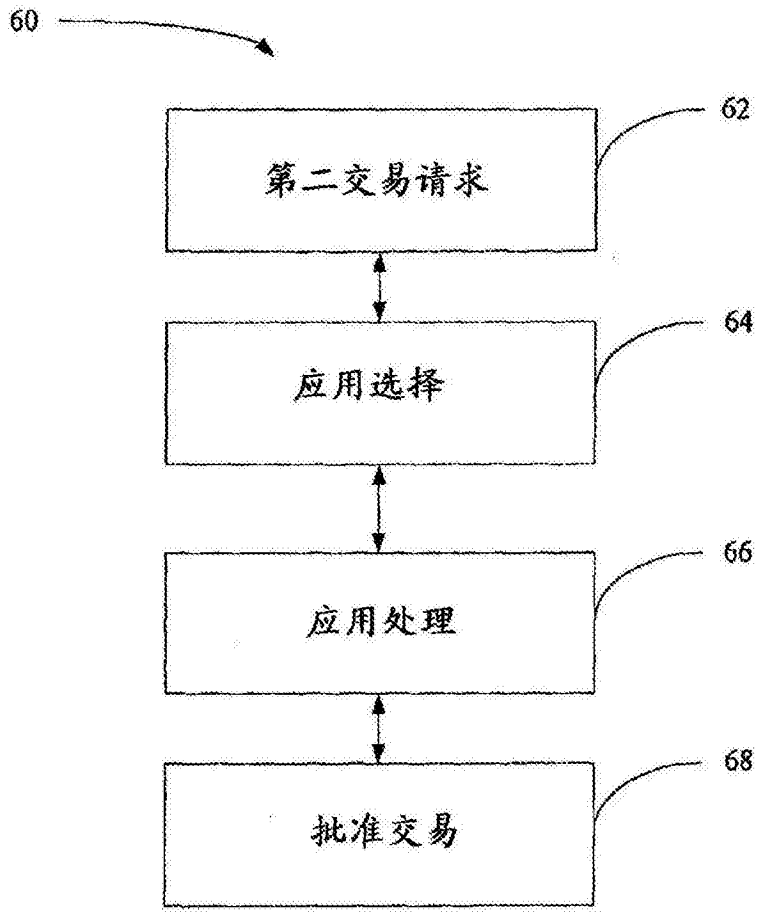


图7